REMARKS / DISCUSSION OF ISSUES

Claims 1-20 are pending in the application. Claims 14-20 are newly added.

The applicant thanks the Examiner for acknowledging the claim for priority, and requests the Examiner's acknowledgment of receipt of certified copies of all the priority documents.

The Examiner is respectfully requested to state whether the drawings are acceptable.

The applicant thanks the Examiner for providing information about recommended section headings in the specification. However, the applicant respectfully declines to add section headings, as they are not required in accordance with MPEP 608.01(a).

Claims are amended for non-statutory reasons: to correct one or more informalities, remove figure label numbers, remove structural elements from method claims, and/or to replace European-style claim phraseology with American-style claim language. The claims are not narrowed in scope and no new matter is added.

The Office action rejects:claims 3, 5, 6, and 8 under 35 U.S.C. 112, second paragraph. The applicant respectfully traverses this rejection. The Office action asserts that p_{diff} and p_{lin} are not defined distinctly in the claims. The applicant respectfully disagrees with this assertion, but in the interest of advancing prosecution in this case, has replaced these mathematical symbols with textual terms.

The Office action rejects

claims 1-2, 4, 6-7, and 9-13 under 35 U.S.C. 103(a) over Lee et al. (USP 6,314,186, hereinafter Lee) and Magliveras et al. (USP 6,038,317, hereinafter Magliveras); and,

claims 3, 5, and 8 under 35 U.S.C. 103(a) over Lee, Magliveras, and the applicant's admitted prior art.

The applicant respectfully traverses these rejections.

Claim 1, upon which claims 2-12 depend, claims a method for cryptographically converting an input data block into an output data block that includes selecting a select permutation from a predetermined set of at least two permutations, and performing a non-linear substitution operation on the input data block based on the select permutation.

The Office action relies upon Magliveras for teaching the selection of a permutation from a set of permutations for use in a substitution operation, and Lee for teaching a non-linear substitution operation based on the selected permutation. The applicant respectfully disagrees with this characterization of Magliveras and respectfully disagrees with the proposed combination of Magliveras and Lee.

Magliveras teaches the formation of a key based upon selected permutations from two logarithmic signatures. The selected permutations are not the basis of a non-linear substitution operation on an input data block, as specifically claimed by the applicant.

Lee teaches a modified DES system, wherein the substitution operation is partitioned into multiple substitution modules, and the input to each substitution module is based on an output of a prior substitution module.

The applicant respectfully maintains that Magliveras's teachings and Lee's teachings are incompatible. Magliveras specifically distinguishes Magliveras's key-generation scheme from DES:

> "It is worth mentioning that our system differs from other known secret key systems such DES, FEAL, or IDEA, in the following way. In the known systems, a key is a certain binary sequence of small length, for example 56, 64, or 128 bits, used as a parameter for an independent encryption function, whereas in our system, the key is a pair of logarithmic signatures which embody the encryption function itself. Thus, the memory required for storing logarithmic signatures in essence corresponds to the memory for implementing encryption functions in the known cryptosystems." (Magliveras, column 38, lines 47-57.)

The applicant respectfully maintains that a combination of the key generation scheme of Magliveras and the DES substitution scheme taught by Lee is not suggested in either Magliveras or Lee, and that such a substitution is not likely to provide a workable encryption system.

The applicant respectfully maintains that the combination of Magliveras and Lee will render the prior art unsatisfactory for its intended purpose, because the permutations selected

for creating a key in Magliveras are not necessarily suitable for use in Lee, and neither Magliveras nor Lee provides any information on how such selected permutations could be used in the substitution boxes of Lee so as to produce an encryption that can be subsequently suitably decrypted.

Further, neither Magliveras nor Lee teaches the desirability of alternating the permutations used in Lee's substitution boxes. The Office action notes that Magliveras teaches the desirability of alternating permutations used for multiplying or factoring elements of permutation groups that are used to generate keys, but such a suggestion is unrelated to a suggestion to alternate permutations in substitution boxes, which are neither multiplying nor factoring elements as taught by Magliveras.

As stated in MPEP 2143:

> "THE PRIOR ART MUST SUGGEST THE DESIRABILITY OF THE CLAIMED INVENTION ... The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). ... The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990)".
>
> also
>
> "THE PROPOSED MODIFICATION CANNOT RENDER THE PRIOR ART UNSATISFACTORY FOR ITS INTENDED PURPOSE
>
> If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification."

Because Magliveras does not teach or suggest the selection of a permutation upon which to base a substitution operation on an input block, and because Magliveras and Lee teach substantially incompatible techniques for cryptographically converting an input block to an output block, the applicant respectfully maintains that claims 1-12 are patentable under 35 U.S.C. 103(a) over Magliveras and Lee.

Additionally, the applicant's dependent claims address techniques and/or criteria for selecting and/or creating the permutations that are not taught or suggested by either Lee or Magliveras.

The Office action cites Magliveras column 1, lines 10-25 and column 73, lines 17-44 for teaching permutations that compensate for cryptographic weaknesses in each other, as claimed in claim 2. The applicant respectfully notes, however, that the cited text of Magliveras is silent with regard to cryptographic weakness or cryptographic strength.

The Office action cites Lee columns 27 and 28 in the rejection of claim 3, upon which claims 4 and 5 depend. The applicant respectfully notes, however, that Lee ends at column 12.

The Office action cites Lee column 2, lines 35-53 for teaching a differential characteristic that has a probability of zero in at least one permutation, as claimed in claim 4, upon which claim 5 depends. The applicant respectfully notes, however, that the cited text of Lee is silent with regard to probabilities of differential characteristics.

The Office action cites Lee columns 27 and 26 in the rejection of claim 6, upon which claims 7 and 8 depend. The applicant respectfully notes, however, that Lee ends at column 12.

The Office action cites Lee column 2, lines 35-53 and column 5, line 66-column 6, line 8 for teaching a linear characteristic that has a probability of ½ in at least one permutation, as claimed in claim 7. The applicant respectfully notes, however, that the cited text of Lee is silent with regard to a linear characteristic that has a probability of ½.

The Office action cites Magliveras column 12, lines 45-67 for teaching selecting the permutation based on an encryption key, as claimed in claim 10. The applicant respectfully notes, however, that the cited text of Magliveras is silent with regard to selecting a permutation based on an encryption key.

The Office action cites Lee column 3, lines 22-34 for teaching selecting a permutation based on one bit of an encryption key, as claimed in claim 11. The applicant respectfully notes, however, that the cited text of Lee is silent with regard to selecting a permutation based on a bit of an encryption key.

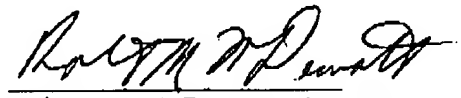
Claim 13 specifically claims a system that includes a cryptographic processor for performing a non-linear operation on the input data block using an S-box based on a selected permutation; wherein, each time before using the S-box, the processor selects the permutation from a stored set of permutations.

The Office action acknowledges that Lee does not teach selecting a permutation before performing the non-linear substitution operation in Lee.

As noted above, Magliveras does not address permutations used for non-linear substitutions. The Office action cites Magliveras's column 73, lines 1-44 for this teaching. The applicant notes, however, that these lines refer to selecting a first permutation and a second permutation, then multiplying these permutations together for form a third permutation. As noted on the following column of Magliveras, at lines 35-41, Magliveras's third permutation is used as a uniquely factorable key for encrypting an input data vector. That is, Magliveras teaches a key creation method based on a selection of permutations, and does not teach selecting a permutation for performing a non-linear substitution operation, as specifically claimed by the applicant.

In view of the foregoing, the applicant respectfully requests that the Examiner withdraw the rejections of record, allow all the pending claims, and find the application to be in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,



Robert M. McDermott, Attorney
Registration Number 41,508
patents@lawyer.com

1824 Federal Farm Road
Montross, VA 22520
Phone: 804-493-0707
Fax: 215-243-7525